REMARKS/ARGUMENTS

This Response is in response to the Final Office Action dated July 29, 2003. Claims 1-39 are pending, and claims 4-6, 17, 19, and 22 have been amended. Claims 1-39 remain pending.

Claims 4-6, 17, 19, and 22 have been amended to provide proper antecedent basis and to correct typographical errors. Accordingly, no new matter has been entered.

The Examiner continues to reject claims 1-39 under 35 USC §102(b) as being anticipated by Chou et al. (US Pat. No. 5,222,133). Applicant respectfully traverses the rejection.

The Examiner's rejection is incorrect for several reasons. First, it is unclear what the Examiner considers analogous to the claimed "encryption key" that is generated within the security device, Chou's first or second key. In some instances, the Examiner indicates that he considers Chou's first key, which is stored on the security device, analogous to the encryption key, and in other instances, the Examiner indicates that he considers Chou's second key, which is entered into the computer, analogous to the encryption key. It is respectfully submitted that only Chou's first key or Chou's second key can be analogous to the encryption key, but not both. For purpose of this discussion, it will be assumed that Chou's first key is analogous to the encryption key because both reside in the security device.

Second, the Examiner mischaracterizes the teachings of Chou. In his rejection, the Examiner states "Chou discloses ... authorizing use of the software on the computer system by generating the encryption key *within* the security device using information supplied from the software." This statement is simply incorrect. The Examiner cites Chou's abstract and col. 1, lines 26-53, to support this contention. The Examiner also cites col. 3, lines 23-39, and col. 4, lines 19-39. In those citations, Chou clearly describes the following:

1) The first key is stored in the plug-in hardware device.

2) The second key is loaded into the computer.

3) The software to be protected is loaded on the computer and the hardware device is plugged into the computer.

4) The software loaded on the computer includes an algorithm for processing a plurality of keys, including the first key.

5) The security device loads the first key onto the computer where the processing of the first and second keys by the algorithm takes place.

6) The processing of the software continues if the processing of the first and second keys derives a control key.

Thus, Chou discloses that the control key is derived on the computer, not on the security device, as the Examiner incorrectly contends. This is an important distinction that the Examiner ignores. In contrast to Chou, the features of the present invention cab be summarized as follows:

1) An initialization vector is bundled with encrypted software in authorization program, which is run on the computer system.

2) A dynamic key is stored in the security device.

3) When a user attempts to use the protected software on the computer system, the initialization vector is passed from the computer system to the security device.

4) The security device uses the two keys to generate an encryption key.

5) The security device transfers the encryption key to the computer system, where it is used to decrypt and execute the encrypted software.

Comparing the above steps with Chou clearly indicates that Chou fails to teach or suggest the claims of the present invention, such as claim 1, for several reasons. First, step (b) of claim recites "authorizing use of the software on the computer system by generating the encryption key *within the security device using information supplied from the software*" (e.g., the initialization vector). Chou, in contrast, teaches that the control key is generated on the computer, rather than in

-15-

the security device. In addition, because the control key is generated on the computer, Chou teaches that the first key is passed from the security device to the computer. Step (b) of claim 1, however, recites that the encryption key is generated "using information supplied from the software," which in the preferred embodiment is the initialization vector. Thus, Chou teaches the opposite of step (b). Instead of passing information from the computer to the security device to generate the encryption key on the security device, Chou teaches passing information from the security device to the computer to generate the control key on the computer.
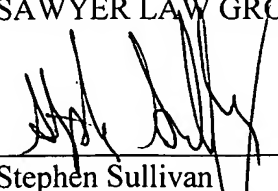
Second, step (c) of claim 1 recites "sending the encryption key from the security device to the computer system for decryption of the software." As stated above, Chou creates the control key on the computer system where the software is authorized. Therefore, step (c) is wholly missing from the teaching of Chou.

Third, the Examiner only address limitations of claim 1 in rejecting independent claims 16, 22, 24, and 39. Because claim 16, 22 and 39 include additional recitations than claim 1, the Examiner failed to set forth how Chou teaches each and every element of claims 16, 22, and 39 to support a proper §102(b) rejection.

Therefore, for the above identified reasons, the present invention as recited in independent claims 1-39 is neither taught nor suggested by Chou. In view of the foregoing, Applicant submits that claims 1-39 are patentable over the cited reference. Applicant, therefore, respectfully requests reconsideration and allowance of the claims as now presented.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

September 29, 2003
Date

Stephen Sullivan
Sawyer Law Group LLP
Attorney for Applicant(s)
Reg. No. 38,329
(650) 493-4540